CEFET/RJ
campus Nova Friburgo

UMA PROPOSTA DE SISTEMA ELETRÔNICO DE VOTAÇÃO COM BLOCKCHAIN

Leonardo Pinto Guilherme

Monografia apresentada ao Curso de Graduação em Sistemas de Informação, do Centro Federal de Educação Tecnológica Celso Suckow da Fonseca, CEFET/RJ Campus Nova Friburgo, como parte dos requisitos necessários à obtenção do certificado de Bacharel em Sistemas de Informação.

Orientador(a): Nilson Mori Lazarin

Rio de Janeiro
Março de 2022

UMA PROPOSTA DE SISTEMA ELETRÔNICO DE VOTAÇÃO COM BLOCKCHAIN

Monografia apresentada ao Curso de Graduação em Sistemas de Informação, do Centro Federal de Educação Tecnológica Celso Suckow da Fonseca, CEFET/RJ Campus Nova Friburgo, como parte dos requisitos necessários à obtenção do certificado de Bacharel em Sistemas de Informação.

Leonardo Pinto Guilherme

Banca Examinadora:

NILSON MORI LAZARIN:72809353115
Assinado de forma digital por NILSON MORI LAZARIN:72809353115
DN: cn=NILSON MORI LAZARIN:72809353115, ou=CEFET-RJ - Centro Fed. Educ. Tecnol. Celso S. Fonseca, o=ICPEdu, c=BR
Dados: 2022.05.26 13:08:49 -03'00'

Presidente, Professor Me. Nilson Mori Lazarin (CEFET/RJ)

gov.br
Documento assinado digitalmente
Carlos Eduardo Pantoja
Data: 30/05/2022 13:13:03-0300
Verifique em https://verificador.iti.br

Professor Dr. Carlos Eduardo Pantoja (CEFET/RJ)

BRUNO POLICARPO TOLEDO FREITAS:00484594028
Assinado de forma digital por BRUNO POLICARPO TOLEDO FREITAS:00484594028
Dados: 2022.05.26 20:06:47 -03'00'

Professor Me. Bruno Policarpo Toledo Freitas (CEFET/RJ)

HELGA DOLORICO BALBI:09599358783
Assinado de forma digital por HELGA DOLORICO BALBI:09599358783
Dados: 2022.05.19 13:39:26 -03'00'

Professora Dra. Helga Dolorico Balbi (CEFET/RJ)

LUIS CLAUDIO BATISTA DA SILVA:07180635707
Assinado de forma digital por LUIS CLAUDIO BATISTA DA SILVA:07180635707
Dados: 2022.05.28 20:11:06 -03'00'

Professor Dr. Luis Claudio Batista da Silva (CEFET/RJ)

Rio de Janeiro

Janeiro de 2022

Ficha catalográfica elaborada pela Biblioteca Central do CEFET/RJ

RESUMO

UMA PROPOSTA DE SISTEMA ELETRÔNICO DE VOTAÇÃO COM BLOCKCHAIN

Considerada um dos principais símbolos da democracia brasileira, a urna eletrônica contribuiu para sufrágios mais ágeis e eliminou muitas das fraudes conhecidas. Por outro lado, também fez crescer a desconfiança do eleitorado com o processo, especialmente do público leigo em tecnologia da informação, sobre o funcionamento das urnas, uma vez que o eleitor não é mais capaz de observar o que acontece com o seu próprio voto. De fato, a auditoria pública do voto é um assunto debatido não apenas por profissionais de tecnologia da informação, como também por juristas, pois os meios disponíveis para auditar o voto comprometem o anonimato da escolha do eleitor, considerado um requisito obrigatório na democracia brasileira. Dado o problema, este trabalho apresenta um modelo de sistema eletrônico de votação que implementa, dentre outras tecnologias, a blockchain e assinaturas cegas para permitir a auditagem pública do voto ao mesmo tempo que o anonimato da escolha do eleitor é garantido durante o processo. A partir de um ambiente com máquinas virtuais, para simular uma seção eleitoral sincronizada com um sistema responsável por coordenar as eleições, foi realizada uma prova de conceito sobre o modelo de sistema, na qual foi possível registrar o voto digital e anônimo de eleitores fictícios e abrir um caminho para a auditoria do voto de cada eleitor.

Palavras-chave: assinatura cega; blockchain; segurança.

ABSTRACT

A PROPOSAL OF AN ELECTRONIC BLOCKCHAIN SYSTEM VOTING

Considered one of the main symbols of Brazilian democracy, the electronic voting machine contributed to more agile voting and eliminated many of the known frauds. On the other hand, it also increased the electorate's distrust with the process, especially the layman in information technology, about the functioning of the polls, since the voter is not able to observe what happens with their own vote. In fact, the public audit of the vote is a subject debated not only by information technology professionals, but also by jurists, since the means available to audit the vote compromise the anonymity of the voter's choice, considered a mandatory requirement in Brazilian democracy. Given the problem, this article presents a proposal for an electronic voting system that implements, among other technologies, the blockchain and blind signatures to allow the public auditing of the vote while the anonymity of the voter's choice is guaranteed during the process. From an environment with virtual machines, to simulate a polling station synchronized with a system responsible for coordinating the elections, a proof of concept was carried out on the system model, in which it was possible to register the digital and anonymous vote of fictitious voters and open a path for the auditing of each voter's vote.

Keywords: blind signature; blockchain; security.

LISTA DE ILUSTRAÇÕES

Figura 1 - Sistema criptográfico simétrico (LAZARIN, 2012) 15
Figura 2 - Sistema criptográfico assimétrico (LAZARIN, 2012) 16
Figura 3 - Etapa do cadastro eleitoral 27
Figura 4 - Passos para realizar a escolha do candidato 28
Figura 5 - Passos para realizar a assinatura cega do voto 28
Figura 6 - Passos para realizar o depósito do voto 29
Figura 7 - Diagrama de blocos do sistema 32
Figura 8 - Geração do par de chaves pública e privada do eleitor 39
Figura 9 - Execução do algoritmo Diffie-Hellman, que gera uma chave global 40
Figura 10 - Geração do par de chaves pública e privada do terminal 40
Figura 11 - Derivação entre as chaves do terminal de depósito e o terminal de escolha 41
Figura 12 - Representação da tela de escolha do candidato pelo eleitor, com nomes fictícios 42
Figura 13 - Assinatura da cédula do voto pelo eleitor, após realizar a sua escolha 42
Figura 14 - Processo de votação do eleitor concluído 43
Figura 15 - Votos dos eleitores registrados no BigChainDB 43

SUMÁRIO

1. Introdução 9
1.1 Motivação 9
1.2 Problema 10
1.2.1 Sob o aspecto jurídico 10
1.3 Objetivo 12
1.4 Contribuição 12
1.5 Estrutura do trabalho 13
2 Referencial Teórico 14
2.1 Criptografia 14
2.1.1 AES 15
2.1.2 RSA 15
2.1.3 Funções hash 16
2.1.4 Diffie-Hellman 17
2.2 Assinatura digital 17
2.3 Assinatura cega 18
2.4 Blockchain 18
2.5 BigChainDB 19
2.6 Processo eleitoral brasileiro 19
2.6.1 Etapa de cadastro eleitoral 20
2.6.2 Etapa da votação 20
2.6.3 Etapa da totalização dos votos 21
3 Trabalhos Relacionados 22
3.1 Uma proposta de sistema eletrônico de votação baseado na blockchain 22
3.2 O futuro da democracia: voto blockchain 23

3.3 Um sistema de i-voting sem papel baseado em assinaturas cegas e anonymous ID 24
4 Modelo proposto 26
4.1 Etapa do cadastro eleitoral 26
4.2 Etapa da votação 27
4.2.1 Escolha do candidato 27
4.2.2 Confirmação de identidade 28
4.2.3 Depósito do voto 29
4.3 Etapa da totalização dos votos 29
5 Implementação 31
5.1 Servidor central da instituição 33
5.2 Terminal de escolha do candidato 34
5.3 Terminal do mesário 36
5.4 Terminal de depósito do voto 37
6 Prova de conceito 39
7 Conclusão 44

1. Introdução

Em um país com aproximadamente 150 milhões de eleitores (BRASIL, 2020), com um território de proporções continentais e características culturais, sociais e geográficas diversas, torna-se um desafio garantir o direito ao voto de cada cidadão brasileiro em função da dificuldade do Estado em garantir a segurança de toda a operação logística do pleito. Diante do cenário, a Justiça Eleitoral do Brasil descontinuou, a partir de 1996, o processo eleitoral manual para torná-lo totalmente informatizado até os dias de hoje. (BRASIL, 2016).

A informatização do processo eleitoral, porém, não é uma exclusividade da democracia brasileira. Países como Índia, Bélgica, Austrália, Espanha e Canadá fazem uso da urna eletrônica, mas cada um à sua própria maneira. Enquanto no Brasil se emprega o equipamento à nível nacional, para eleger representantes de todos as esferas de governo, na Espanha, por exemplo, usa-se apenas a nível municipal, em algumas cidades. (KUMAR e BEGUM, 2012).

Com um processo eleitoral desenvolvido, especialmente, para a realidade brasileira, a digitalização do sufrágio teve como objetivo não apenas aumentar a segurança das votações, mas também reduzir tempo, recursos e custos. Através da urna eletrônica, foi possível garantir o sigilo da escolha do eleitor, implementar múltiplos mecanismos de segurança para impedir adulterações do voto e agilizar o processo de apuração do voto. (BRASIL, 2016).

Entretanto, o sufrágio digitalizado, que agora exige conhecimentos técnicos, obscureceu a sua compreensão para o eleitorado e gera desconfianças que permitem que o senso comum desenvolva teorias da conspiração e propague desinformação, o que, consequentemente, perturba o processo eleitoral.

1.1 Motivação

Enquanto a tecnologia da informação cumpre com o seu papel de apoiar em atividades que, antes, eram manualmente inviáveis de serem executadas,

obscurece, ao ser humano, etapas críticas de um processo como o sufrágio. Uma das etapas que tem levantado questionamentos, conforme aprofundados nos tópicos seguintes, é a auditoria do voto. (OLIVEIRA, 2021).

O debate se trata em alcançar um nível satisfatório de transparência do processo de auditoria aos cidadãos que participam do pleito, isto é, colocar à prova se o voto depositado ao eleitor corresponde àquele que está registrado na urna. Porém, a transparência, em nenhum momento, pode comprometer o anonimato do voto do eleitor e, ao mesmo tempo, também não é simples a tarefa de definir um nível satisfatório de transparência.

Embora a urna eletrônica esteja em uso em outros países do mundo, este trabalho mantém como foco, unicamente, o cenário brasileiro.

1.2 Problema

O desenvolvimento de um processo eleitoral político, mesmo que totalmente informatizado, não é uma atribuição exclusiva da tecnologia da informação. As regras do processo estão definidas na Constituição Federal, escrita por legisladores e juristas – embora as demandas políticas também podem influenciar o texto. Outros requisitos são definidos por técnicos da Justiça Eleitoral, mas sempre em consonância com a Constituição.

Devido à complexidade do processo, os casos de sucesso em outros países nem sempre podem ser replicados no cenário doméstico ou vice-versa. Caso contrário, a sua implementação pode exigir debates políticos e modificações que inviabilizam o projeto original. Isso ocorre porque os desafios e problemas variam de um país para o outro.

Para os profissionais em tecnologia da informação responsáveis pelo processo, cabe apenas oferecer as soluções que estejam adequadas às demandas estabelecidas pelos outros atores.

1.2.1 Sob o aspecto jurídico

O trabalho apresentado por Marcacini e Barreto Junior (2019) apresenta

uma análise sobre as problemáticas envolvidas em um processo eleitoral eletrônico. Os autores discutem sobre a impossibilidade de oferecer um sufrágio que seja, ao mesmo tempo, (a) 100% digital, (b) publicamente auditável e (c) anônimo em relação ao voto.

Em sua análise sobre o sigilo, os autores mencionam o artigo 14, da Constituição Federal que garante ao eleitor o voto secreto. O objetivo do voto secreto é assegurar a liberdade do eleitor segundo a sua vontade própria, bem como protegê-lo de pressões em seu círculo profissional e familiar ou de qualquer influência que, de alguma forma, possa intimidá-lo.

O sigilo, porém, deve ser completo, ou seja, de nenhuma maneira deve ser possível identificar quem votou em quem. Para exemplificar, os clientes de instituições bancárias possuem direito ao sigilo, mas as operações não são sigilosas para o próprio banco ou cliente, bem como ocorre com o sigilo das telecomunicações, o sigilo profissional ou o sigilo judicial.

Para aprofundar na discussão sobre o sigilo, pode-se utilizar o exemplo das instituições bancárias, citado no parágrafo anterior. Júnior (2016), argumenta em seu artigo sobre o relativo sigilo bancário dos contribuintes brasileiros perante as autoridades fiscais que, com o amparo da lei e por diferentes razões, entre as quais, a identificação e prevenção de fraudes financeiras, acessam os dados bancários dos residentes do país. Além disso, o Brasil também é signatário de convenções internacionais para o intercâmbio de informações fiscais. Em qualquer caso, a maneira como as informações bancárias são utilizadas é habitualmente reavaliada em decretos presidenciais e discutida no Supremo Tribunal Federal.

No caso do processo eleitoral brasileiro, mais do que um voto sigiloso, busca-se um voto anônimo, em que nem o próprio eleitor deve ser capaz de identificar o seu voto entre os outros depositados na mesma urna.

Entretanto, os requisitos para garantir o anonimato do voto prejudicam a transparência do processo e, consequentemente, a auditabilidade da votação, uma vez que o resultado da apuração deixa de ser publicamente demonstrado. Por isso, os autores mencionam o voto impresso como uma das soluções, mas reconhecem os inúmeros relatos de falhas confirmadas acerca dos sistemas de

votação não eletrônicos.

Por fim, a conclusão dos autores é que apenas dois dos três requisitos quaisquer, mencionados anteriormente, podem ser cumpridos.

1.3 Objetivo

Para este trabalho, foi desenvolvido um modelo de sistema eletrônico de votação capaz de garantir o anonimato da escolha do eleitor e a segurança da informação de toda a infraestrutura utilizada na proposta. Cabe ressaltar que não compete a este trabalho a comparação, análise ou julgamento do funcionamento da urna eletrônica atualmente em uso no Brasil, tampouco a elaboração de um novo processo eleitoral ou análise de questões não relacionadas aos requisitos técnicos do escopo. Entretanto, alguns atributos do processo e do sistema eleitoral brasileiro são apresentados neste trabalho e aproveitados na proposta, de modo que o modelo de sistema desenvolvido esteja o mais próximo possível da realidade atual.

O sistema apresentado se limita apenas ao escopo da segurança da informação do processo de votação e a sua infraestrutura envolvida, suficiente para realizar a prova de conceito do funcionamento deste sistema. Portanto, não se trata de uma aplicação robusta, projetada para um usuário final. Como resultado, o sistema em questão possibilita um mecanismo de validação do voto pela parte do eleitor e um novo meio de se auditar as votações, tal como discutido por Marcacini e Junior (2019).

1.4 Contribuição

Como contribuição e diferencial aos trabalhos mencionados no Capítulo 3 (Adiputra *et al.* (2018), que implementa a blockchain em um sistema de votação online, Osgood (2016), que apresenta um sistema híbrido de votação, também com a blockchain e Barros e Pimenta (2018), que propõem um sistema de votação baseada em assinaturas cegas com um aplicativo móvel), este trabalho apresenta uma proposta de sistema eletrônico de votação, presencial, em que

se busca utilizar, mutuamente, as tecnologias experimentadas nos trabalhos citados, em especial, a *blockchain* e as assinaturas cegas. Entretanto, também implementa outras tecnologias e ferramentas, conforme mencionadas no Capítulo 2. Por outro lado, descarta o uso da Internet nas seções eleitorais durante o processo de votação.

1.5 Estrutura do trabalho

No Capítulo 2, descreve-se o referencial teórico que abrange o modelo proposto, tanto em relação às tecnologias e ferramentas, como em relação ao processo eleitoral brasileiro.

No Capítulo 3, são abordados trabalhos relacionados, que também contribuíram para o desenvolvimento do modelo de sistema da proposta.

No Capítulo 4, é apresentada a proposta deste trabalho.

No Capítulo 5, é apresentada a implementação e estrutura da proposta para a prova de conceito.

No Capítulo 6, apresenta-se a prova de conceito.

No Capítulo 7, estão as considerações finais.

2 Referencial Teórico

Neste capítulo, são apresentadas as tecnologias e ferramentas utilizadas na proposta, além de uma breve explicação sobre o funcionamento do processo eleitoral brasileiro.

2.1 Criptografia

A criptografia é o conceito utilizado em uma informação que se deseja esconder, de modo que apenas um grupo limitado de pessoas seja capaz de revelar e interpretar a informação criptografada. Em rede de computadores é utilizada para tornar uma comunicação ilegível.

Os sistemas criptográficos podem ser caracterizados em três dimensões independentes (STALLINGS, 2015):

- **o tipo das operações usadas para transformar texto claro em texto cifrado**, no qual o algoritmo de encriptação substitui os elementos de um texto legível por outros elementos mapeados ou são rearranjados dentro do próprio texto.
- **o número de chaves usadas**, que podem configurar uma encriptação simétrica, quando o emissor e receptor possuem a mesma chave ou assimétrica, quando as chaves destes atores são distintas.
- **o modo em que o texto é processado**, isto é, em cifra de blocos ou cifra em fluxo que definem, respectivamente, se os elementos do texto são processados em blocos ou continuamente.

Um sistema criptográfico pode implementar diferentes técnicas, especificações, protocolos e funções de acordo com a necessidade do programador e a criticidade de uma informação trafegada em uma rede qualquer. Alguns dos ferramentais mais usados em criptografia, que também são aproveitadas neste trabalho, estão definidos nos subtópicos a seguir.

2.1.1 AES

Advanced Encryption Standard (AES) é um algoritmo de cifra simétrica com a função encriptar e desencriptar uma informação. O algoritmo pode tanto transformar uma informação em texto cifrado, inelegível, como revertê-lo para um texto plano, na sua forma original. Com a cifra simétrica, a chave de decifração é a mesma ou pode ser obtida a partir da chave de decifração.

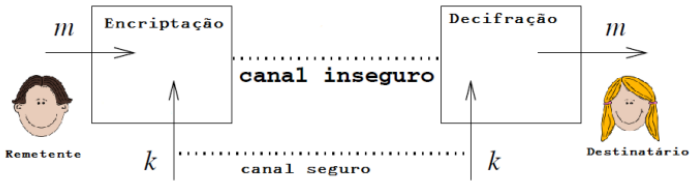

Figura 1 - Sistema criptográfico simétrico (LAZARIN, 2012)

O algoritmo processa bloco de dados de 128 bits, como entrada, e com chaves criptográficas de 128, 192 ou 256 bits, embora a unidade de processamento do AES seja em bytes. Com estes três tamanhos de chave, o algoritmo pode ser referenciado como AES-128, AES-192 e AES-256. (DWORKING *et al.*, 2001).

O AES foi publicado em 2001, no Instituto Nacional de Padrões e Tecnologia, nos Estados Unidos, e adotado pelo governo deste país. A sua eficiência contribuiu para que o Data Encryption Standard (DES), outro algoritmo de cifragem amplamente utilizado até então, perdesse relevância, quando comparado ao AES. (STALLINGS, 2015).

2.1.2 RSA

RSA, acrônimo originado pelas iniciais dos seus inventores Rivest, Shamir e Adleman, é um dos primeiros e mais populares sistemas criptográficos para assinatura digital. O sistema consiste em um par de chaves pública e privada para encriptar e desencriptar uma informação. O sistema utiliza a fatoração do produto de dois números primos grandes, que o torna em um dos mais seguros e difíceis de quebrar. (ASHIDANI; BARBAR, 2008).

Este algoritmo faz uso da chave assimétrica – diferentemente da chave

simétrica, que faz uso de uma única chave para codificar e decodificar dados, a chave assimétrica utiliza outras duas: a pública e privada para, respectivamente, codificar e decodificar a informação. Com uma chave pública, pode-se saber quem enviou uma informação codificada, enquanto com uma chave privada pode decodificar a informação recebida. (STALLINGS, 2015).

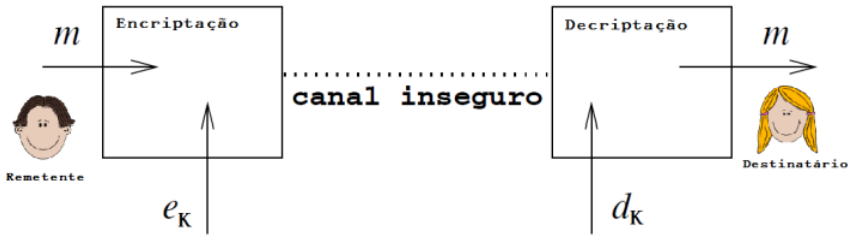

Figura 2 - Sistema criptográfico assimétrico (LAZARIN, 2012)

2.1.3 Funções hash

Uma função *hash* é um algoritmo matemático de criptografia responsável por receber um ou mais elementos de entrada, de tamanho variável, e transformá-los em um outro elemento que, geralmente, é uma cadeia de caracteres, de tamanho fixo. O resultado deste processo é conhecido como *message digest*. Qualquer alteração na cadeia de caracteres aplicada a uma função *hash* resulta, com grande probabilidade, em um *message digest* distinto. Por esse motivo, uma função *hash* é útil para conferir a integridade de um arquivo (DANG, 2015).

Existem vários algoritmos de função *hash* atualmente em uso, como o MD5 (de 128 bits) e SHA-1 (de 160 bits), sendo que esta última, por sua vez, possui outras versões, como o SHA-256 (de 256 bits) e SHA-512 (de 512 bits). (DANG, 2015).

A escolha por uma função ou outra é de responsabilidade do programador, que deve levar em consideração fatores como a criticidade da informação tratada.

Para qualquer função *hash*, todas possuem as seguintes características: geram um *digest* único e exclusivo para uma determinada massa de dados; o resultado gerado é irreversível, isto é, a mensagem original criptografada não

pode ser recuperada; e o valor do resultado tem um tamanho fixo de bits, a depender da função utilizada.

Computacionalmente, para um atacante é inviável encontrar um objeto de dados a partir de um *digest* de função *hash* pré-especificado. Dadas suas características, algumas aplicações fazem uso dessa função, como autenticação de mensagens, assinaturas digitais e arquivos de senha de mão única. (STALLINGS, 2015).

2.1.4 Diffie-Hellman

Diffie-Hellman é um algoritmo criptográfico que permite a troca de chaves entre usuários através de um canal potencialmente inseguro, ou seja, mesmo sob ataques. Os protocolos que fazem uso deste algoritmo não implementam qualquer técnica de cifragem aos dados, mas apenas estabelece um canal seguro para que chaves sejam trocadas de uma ponta a outra.

O algoritmo se baseia em logaritmos discretos, considerados difíceis de calcular, para alcançar a sua eficácia em relação a segurança. Diffie-Hellman não realiza qualquer tipo de autenticação dos usuários participantes no processo de troca de chaves, o que torna a comunicação sensível a ataques como *man-in-the-middle*, isto é, interceptação por terceiros. Por essa razão, a segurança pode ser complementada com assinaturas digitais. (STALLINGS, 2015).

O nome do protocolo é originário dos seus inventores Whitfield Diffie e Martin Hellman. Os primeiros exemplos práticos do método foram publicados no artigo New Directions in Cryptography, em 1976.

2.2 Assinatura digital

Assinatura digital é uma técnica computacional que substitui uma assinatura manuscrita em um documento de papel, isto é, possui a finalidade de certificar a origem de um conteúdo eletrônico e garantir a integridade dos dados assinados.

Com um mecanismo de comunicação, para proteger os usuários de um

ataque de terceiro, um documento pode ser digitalmente assinado com uma chave privada, que deve estar em posse do assinante e restringida por senha, enquanto uma chave pública correspondente permite a comprovação da autenticidade do documento em questão. Esta comprovação pode ser realizada por qualquer pessoa, desde que se tenha a chave pública. (STALLINGS, 2015).

Quando necessário, mais de uma pessoa pode assinar o mesmo documento, tal como ocorre com documentos físicos. Para isso, cada uma deve possuir o seu próprio par de chaves pública e privada.

2.3 Assinatura cega

Uma assinatura cega (também conhecida como *blind signature*, em inglês) é uma assinatura digital, tal como descrito no tópico anterior, porém com a diferença de que as partes assinam um documento com o conteúdo oculto, ou seja, desconhecem as informações contidas no documento. Por outro lado, as partes que o assinam podem ser conhecidas normalmente, pois o objetivo é apenas preservar o sigilo do teor do documento.

Este tipo de assinatura é útil quando o documento em questão contém informações confidenciais ou que não podem ser acessadas por outras pessoas. O conceito da assinatura cega foi apresentado por Chaum (1983) e já foi utilizado em outros estudos relacionados à segurança da informação em eleições – um deles está mencionado no Capítulo 3.

2.4 Blockchain

Blockchain é uma rede descentralizada que permite o registro distribuído de transações. Funciona como um livro-razão, em que cada novo registro é replicado em diferentes dispositivos que se responsabilizam por validá-lo consensualmente e, consequentemente, podem ser rastreados em tempo real. Desta maneira, torna-se inviável tentativas de adulteração dos registros, uma vez que qualquer inconsistência transacional identificada por um dos nós é passível de rejeição. (XU *et al.*, 2019).

Uma das aplicações mais notórias desta tecnologia é o Bitcoin, uma criptomoeda digital idealizada por Nakamoto (2008), que garante transações financeiras mais seguras através de uma chave criptografada gerada em cada registro que deve ser validada por outros servidores da rede. Esta aplicação foi, justamente, a que concebeu a blockchain.

2.5 BigChainDB

O BigChainDB é um sistema gerenciador de banco de dados não-relacional, *open source* e baseado em MongoDB. Este sistema implementa a blockchain, uma tecnologia que permite o registro descentralizado de transações imutáveis e anônimas. O banco de dados pode ser instalado, configurado e executado somente em sistemas operacionais baseados em Linux. A primeira versão do BigChainDB foi lançada em 2016 e atualmente se encontra na versão 2.0. (BIGCHAINDB GMBH, 2018).

Com o BigChainDB, pode-se realizar consultas de inserção e leitura dos dados registrados, mas não há a possibilidade de removê-los nem os editar, uma vez que os dados estão registrados na blockchain. Cada registro possui um identificador único formado por uma cadeia de 64 caracteres.

Devido às características descritas, o BigChainDB foi escolhido para este estudo, de modo a garantir maior segurança da informação, como a impossibilidade de adulterar os votos já registrados pelos eleitores.

2.6 Processo eleitoral brasileiro

Para compreender a proposta deste trabalho, este capítulo apresenta um breve conhecimento sobre o processo eleitoral brasileiro, elaborado pelo Tribunal Superior Eleitoral, que o define em diversas etapas, entre as quais, estão o cadastro eleitoral, a votação e a totalização dos votos. O processo eleitoral brasileiro não se limita a estas etapas, mas para este estudo, são as mais relevantes. A partir do processo explicitado nos tópicos a seguir, pôde-se elaborar o modelo de sistema proposto com atores, fases e atributos consoantes

ao processo atual.

2.6.1 Etapa de cadastro eleitoral

O brasileiro que atingiu a maioridade eleitoral e está obrigado a votar deve, em até seis meses antes da data da eleição, alistar-se no cartório eleitoral mais próximo da sua casa. Para efetuar o cadastro, o eleitor deve apresentar um documento oficial com foto e comprovante de residência. Durante o cadastro, também é realizada a coleta biométrica dos dedos do cidadão. Estas informações são armazenadas sigilosamente no cadastro do eleitor. (BRASIL, 2015a).

Uma vez confirmados os dados, o eleitor é inscrito na Justiça Eleitoral e recebe um novo documento: o título de eleitor, que serve para provar que o cidadão está inscrito em determinada zona eleitoral.

Desde abril de 2020, em função da pandemia da COVID-19, o Tribunal Superior Eleitoral possibilita a emissão do título de maneira on-line, por meio do sistema Título Net, que pode ser acessado através do computador e dispositivos móveis. (BRASIL, 2020).

2.6.2 Etapa da votação

Durante o período das votações, o eleitor devidamente inscrito na Justiça Eleitoral deve se dirigir para a seção eleitoral indicada em seu título. Em sua seção, o eleitor deve apresentar o título junto a um documento oficial com foto ao mesário para a conferência das informações, além da leitura biométrica dos dedos. Os dados são conferidos no terminal do mesário e, após a confirmação, o eleitor deve assinar o caderno de votação e, então, recebe o comprovante de comparecimento.

Nesta mesma ocasião, o mesário libera o terminal do eleitor para o registro do seu voto. Em seguida, o eleitor deve se dirigir até a cabine de votação, onde está a urna eletrônica para digitar o número do seu candidato para o cargo indicado e confirmar o seu voto. Quando finalizado, o eleitor deve se retirar da

seção. (BRASIL, 2015c).

2.6.3 Etapa da totalização dos votos

Esta é a etapa que ocorre após a finalização das votações nas seções eleitorais. Os dados registrados na urna são assinados digitalmente, criptografados e armazenados em uma mídia de resultado. Logo, gera-se um boletim de urna, isto é, a divulgação do resultado das votações da urna em questão.

A totalização dos votos inicia, de fato, quando a mídia de resultado é encaminhada para um local de transmissão dos dados, que devem ser recebidos pelo Tribunal Regional Eleitoral, que, por sua vez, é responsável por fazer a soma dos votos de todos os boletins de urna. Logo, os resultados das eleições são divulgados pelo próprio Tribunal.

O Tribunal Superior Eleitoral esclarece que os votos nulos e em branco não são considerados na soma dos votos válidos. (BRASIL, 2015b).

3 Trabalhos Relacionados

Nesta seção, são apresentados os trabalhos relacionados ao tema e que contribuíram para o desenvolvimento da proposta.

3.1 Uma proposta de sistema eletrônico de votação baseado na blockchain

Adiputra *et al.* (2018) destacam as problemáticas do voto físico, desde o deslocamento do eleitor da sua casa até o depósito do seu voto na urna de um colégio eleitoral. Como exemplo, menciona o declínio da taxa de participação das pessoas em eleições de alguns países e as cenas de violência no referendo pela independência da Catalunha, em 2017. Por essas razões, os autores entendem que o sufrágio através da Internet é uma solução promissora.

Baseado no modelo de votação implementado na Estônia, os autores propõem um processo eleitoral online, porém reconhecem os problemas de segurança envolvidos. A solução então é o uso da tecnologia blockchain. Neste modelo, a comissão eleitoral cria o um único par de chaves pública e privada, para encriptar e desencriptar os votos, enquanto cada eleitor também deve criar o seu próprio par de chaves pública e privada, de modo a conferir a autenticidade do documento que identifica o eleitor - a chave pública do eleitor deve ser guardada secretamente. O voto já encriptado é enviado para uma rede blockchain, de modo que cada voto enviado é um novo bloco na rede. Desta maneira, qualquer eleitor pode conferir que um voto foi, de fato, enviado.

Esse esquema diminui a possibilidade de adulterações não detectadas, uma vez que um agente malicioso precisaria desencriptar o voto trafegado em rede, adulterá-lo e novamente encriptá-lo, além de que a hash do bloco na rede seria modificada. Ao fim da votação, todas as chaves públicas são destruídas e qualquer eleitor, então, pode começar a contar os votos.

Este presente trabalho também propõem um sistema de votação baseado em blockchain, rede onde deve ser registrado o voto de cada eleitor, para garantir a inalterabilidade dos votos, seja antes ou depois da sua apuração, de modo que seja possível uma eventual recontagem dos votos após o término das

votações. Porém, o presente trabalho descarta o uso de sistemas online no processo de votação.

3.2 O futuro da democracia: voto blockchain

Osgood (2016) destaca que o modelo de urna mais comum do mundo é aquele que utiliza cédulas de papel, o qual tem a vantagem de ser mais barato, porém não é escalável e depende de profissionais que o manuseie corretamente e honestamente. Ao mesmo tempo, existem as urnas eletrônicas que abrem brechas para vulnerabilidades que podem ser exploradas por governos ou outras organizações de influência. Dado o problema, o blockchain se apresenta como uma tecnologia de oferecer sigilo absoluto ao eleitor ao mesmo tempo que também previne fraudes digitais explicitadas no estudo.

O autor apresenta, em seu artigo, uma breve análise dos fundamentos do blockchain e exemplos das suas aplicações em sistemas de votação.

Entre as principais aplicações de sistemas de votação em blockchain estão:

- Votebook
- Follow My Vote
- VoteWatcher

A proposta está baseada no modelo Votebook e VoteWatcher, que utilizam um sistema híbrido de votação, com uma urna eletrônica e outra com cédula de papel. As cédulas de papel devem conter um QR Code, que deve ser escaneado pela urna. Logo, o voto é enviado para uma rede blockchain local. Ao fim da votação, esses votos são enviados a um DVD, que, junto com as cédulas de papel, devem ser guardadas em local seguro. Então, realiza-se a contagem dos votos de cada máquina. Caso todos os votos sejam considerados válidos, os dados entram em uma nova rede de blockchain com outras máquinas.

Como já mencionado na introdução deste trabalho, a discussão do problema não está limitada em oferecer o registro seguro do voto, mas também em garantir votos anônimos e totalmente digitais, de modo que também seja possível auditá-los. O sistema híbrido de votação de Osgood (2006), que

imprime uma cédula de papel viola a condição dos votos 100% digitais. Entretanto, a proposta de registrar os votos na rede blockchain é utilizada como parte da solução deste trabalho.

3.3 Um sistema de i-voting sem papel baseado em assinaturas cegas e anonymous ID

Baseando-se no conceito de assinaturas digitais, em que se aplica um par de chaves pública e privada em um documento para atestar sua autenticidade, Barros e Pimenta (2018) propõem um sistema de votação eletrônico com assinaturas cegas.

Uma assinatura cega é definida como uma assinatura digital em que o assinante não possui conhecimento sobre o conteúdo do documenta que assina. Neste caso, a autoridade certificadora da assinatura não é capaz de acessar o conteúdo do documento, mas deve ser capaz de identificar quem o assinou, para evitar ataques de impersonação.

Na proposta dos autores, utiliza-se a assinatura digital duplamente cega para impedir a quebra do anonimato do voto, de modo que nem o próprio eleitor deve ser capaz de identificar o seu voto. Para isso são utilizados dois servidores: um de autenticação do eleitor para assinatura dos votos e outro para coleta e contagem dos votos. Estes dois servidores não se comunicam entre si.

O design da eleição se divide em quatro fases:

- **preparação da eleição**: um par de chaves pública e privada e gerado para cada servidor, junto com o seu respectivo certificado. No servidor de autenticação, estarão os dados de todos os eleitores aptos a votar. Os eleitores, por sua vez, instalam e se registram no aplicativo móvel da eleição. Este registro estará associado com as suas informações já registradas no banco de dados
- **requisição das urnas e identificações anônimas**: conectado ao aplicativo, o eleitor deve gerar sua identificação anônima (*anonymous ID*). Logo, o servidor gera uma assinatura cega e a

envia para o eleitor junto com o seu voto digital.

- **segunda requisição de identificação anônima**: o eleitor se autentica no servidor de votação, então, gera uma assinatura randômica, que oculta a chave pública do servidor de autenticação. Nesta fase, a autoridade eleitoral publica a lista das assinaturas randômicas para que cada eleitor possa conferir se a sua está presente.
- **depósito e assinatura do voto**: o eleitor já pode depositar o seu voto através da aplicação, que gera uma assinatura cega e computa o seu voto cego.

Graças à combinação do *anonymous ID* com as assinaturas cegas, ao fim do período de votação, os votos podem ser apurados e auditados sem qualquer possibilidade de identificar quem votou em quem.

A proposta do uso de assinaturas cegas nas votações vai ao encontro ao apresentado no Capítulo 4 deste trabalho (onde está definido o modelo proposto), mas, para o sufrágio, não se utiliza um aplicativo no dispositivo móvel, dada a dificuldade de garantir a segurança da informação de cada eleitor, além das possibilidades de brechas que devem ser identificadas e corrigidas. Em vez disso, as assinaturas cegas são utilizadas no terminal do eleitor, na seção eleitoral, isto é, em um ambiente controlado pela comissão eleitoral.

4 Modelo proposto

Este modelo, que está baseado no processo eleitoral brasileiro, conforme descrito no Capítulo 2, propõe a capacidade do eleitor de validar o seu próprio voto, antes do seu depósito na urna, além de oferecer instrumentos para uma auditoria pública das eleições, de modo a aumentar a transparência do processo, que pode contribuir para a maior confiança do eleitor no sufrágio.

Para que se implemente o sistema eletrônico de votação proposto neste trabalho, algumas modificações ao processo inspirado seriam necessárias, conforme explicitadas no próximo tópico.

Outras etapas do processo eleitoral brasileiro, não abordadas neste estudo, como a logística e a preparação das eleições podem ser mantidas ou ajustadas ao modelo proposto, conforme a necessidade.

4.1 Etapa do cadastro eleitoral

Para esta etapa, a modificação a ser feita é acrescentar um passo para gerar um par de chaves pública e privada junto à emissão do título de eleitor, em um dispositivo removível (que será definido neste trabalho como cartão eleitoral), que deve ser retirado na junta eleitoral mais próxima à residência do eleitor.

Para a chave privada, uma senha é atribuída a ela e deve estar em posse do eleitor, armazenada confidencialmente com ele próprio. No caso da chave pública, deverá estar armazenada no banco de dados do sistema central (na Figura 3, definido como Sistema de Registro de Eleitores), junto às demais informações do eleitor. Estas chaves serão utilizadas na etapa de votação.

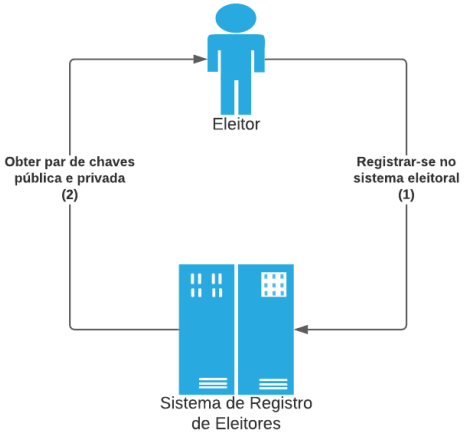

Figura 3 - Etapa do cadastro eleitoral

A Figura 3 representa os primeiros passos do eleitor nesta proposta. Ao fim, o eleitor deve receber, junto ao seu documento, caso ainda não o tenha ou esteja desatualizado, um cartão eleitoral contendo o seu certificado eleitoral (a chave privada) para usá-lo no dia das eleições.

4.2 Etapa da votação

Esta etapa possui as modificações mais abrangentes. Cada passo desta etapa pode envolver atores e dispositivos diferentes, em contextos diferentes. Por isso, o fluxo da etapa de votação foi dividido em três partes, composto por oito passos, ao todo, conforme descritos nos subtópicos seguintes. Entretanto, todas as atividades desta etapa ocorrem em um único ambiente: na seção eleitoral do eleitor, presencialmente.

4.2.1 Escolha do candidato

Primeiramente, o eleitor se dirige a um terminal de escolha do candidato, da seção eleitoral, conforme previamente indicado em seu título de eleitor, para selecionar o(s) candidato(s) para o(s) cargo(s) em disputa. Uma vez confirmada, o eleitor recebe uma cédula digital do seu voto, registrada em seu cartão eleitoral, que sinaliza a confirmação da sua escolha – esta cédula não contém o voto eleitor. Em seguida, o eleitor deve retirar o seu cartão eleitoral do terminal.

A Figura 4 representa os passos do eleitor, quando as votações estão abertas. O banco de dados, conectado ao servidor, representa as informações essenciais que devem ser previamente registradas, antes das eleições, como os dados do eleitor na seção eleitoral em questão e os dados dos candidatos em disputa.

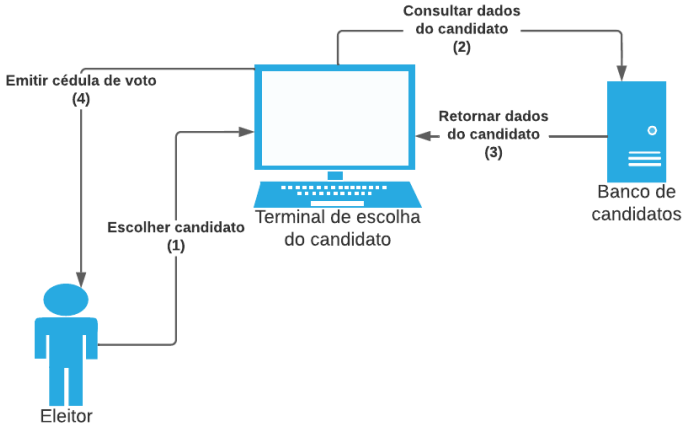

Figura 4 - Passos para realizar a escolha do candidato

4.2.2 Confirmação de identidade

Ainda na seção eleitoral, o eleitor deve se dirigir ao mesário e inserir o cartão eleitoral em seu terminal. O mesário, por sua vez, deverá verificar a identidade do eleitor e assinar, cegamente, a sua cédula do voto. Em seguida, o eleitor deve retirar o seu cartão eleitoral. Cabe ressaltar que a assinatura cega é, justamente, o passo que garante ao eleitor o anonimato da sua escolha.

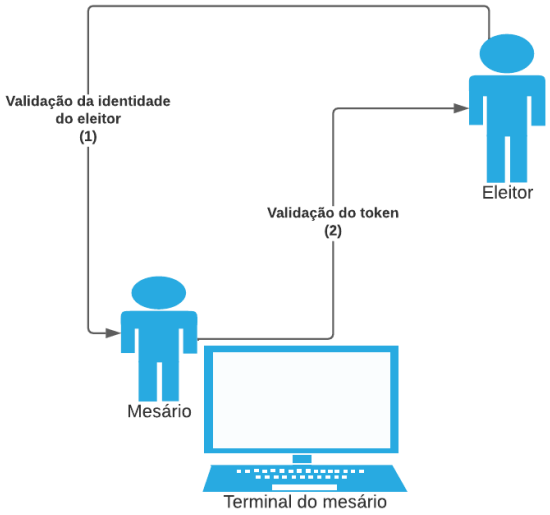

Figura 5 - Passos para realizar a assinatura cega do voto

Caso nenhuma inconsistência seja encontrada com os dados ou a assinatura do eleitor, o mesário pode autorizar que o eleitor prossiga ao passo de depósito do voto.

4.2.3 Depósito do voto

Por fim, o eleitor deve seguir ao terminal de depósito do voto, onde o seu cartão eleitoral deve ser inserido, mais uma vez, e confirmar a assinatura do mesário. Se nenhuma mensagem de erro for indicada na tela (falha na validação da assinatura), o voto será depositado na urna.

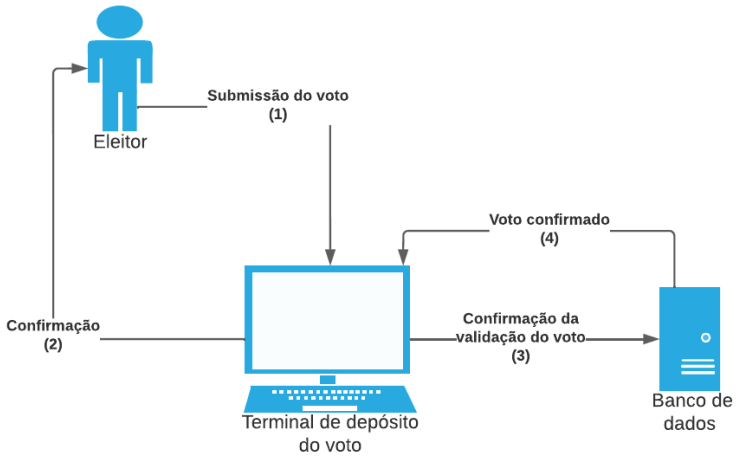

Figura 6 - Passos para realizar o depósito do voto

O banco de dados mencionado na Figura 6 é o BigChainDB, o qual manterá registrado os votos dos demais eleitores que depositaram o voto nesta mesma urna.

4.3 Etapa da totalização dos votos

O depósito do voto na urna representa o seu registro na *blockchain*, com o BigChainDB. Neste banco de dados, apenas será registrado o candidato que foi votado por cada eleitor. Nenhuma informação do eleitor é registrada no banco de dados. Junto ao voto, também é registrada a data e hora que o registro foi inserido no banco de dados, além de um *message digest*. Como mencionado no Capítulo 3, sobre o BigChainDB, este é um identificador único do registro.

A totalização dos votos será feita diretamente na urna de depósito do voto em questão após a finalização da votação. Os dados não serão assinados digitalmente, criptografados, armazenados em arquivo de mídia e transmitidos para um servidor central, tal como ocorre no cenário real, devido a que o estudo de caso trata apenas de uma seção eleitoral, com uma única urna de depósito.

5 Implementação

Para implementar o modelo proposto, foram configuradas quatro máquinas virtuais para simular:

- um servidor central da instituição autárquica eleitoral;
- um terminal do mesário;
- um terminal de escolha do candidato do eleitor e
- um terminal de depósito do voto do eleitor.

Os três terminais são usados para representar as urnas de uma seção eleitoral, enquanto o servidor central é o responsável por armazenar os dados de todos os eleitores e gerenciar as eleições.

Cada uma destas máquinas foi configurada com o sistema operacional Ubuntu, uma distribuição Linux, na versão 20.04.3 LTS. A linguagem de programação utilizada foi o Python, na versão 3.8, que, por sua vez, fez uso da biblioteca *os*[1], para enviar comandos ao sistema operacional. O sistema foi programado em arquivos de *script* e executados pelo usuário através da sua chamada no terminal, sendo este a interface do usuário.

Os comandos submetidos ao terminal, em sua grande maioria, fazem parte do pacote OpenSSL[2], um ferramental de administração de bibliotecas relacionadas com a criptografia, como funções hash, assinaturas digitais, Diffie-Hellman, entre outros.

A sequência de comandos do processo é viável de ser executada manualmente, mas para desenvolver a implementação com maior produtividade, agilidade e organização, optou-se por automatizá-la. Estes *scripts*, em Python, não fazem nada mais do que enviar comandos ao terminal. Em alguns casos, antes de executar o comando, o *script* pode precisar buscar arquivos em outra máquina, em um processo que simula o uso de um cartão eleitoral. Por isso,

---

[1] https://docs.python.org/3/library/os.html

[2] https://www.openssl.org/

também se utilizou conexão de rede apenas com o objetivo de reduzir esforço manual neste processo, mas, em um cenário real, tal uso poderia ser integralmente descartado.

Especialmente na máquina virtual que simula um terminal de depósito do voto do eleitor, também foi configurado o banco de dados BigChainDB, para o registro dos votos e o MongoDB Compass[3], um software que oferece uma interface gráfica para gerenciamento de bancos de dados baseados em MongoDB, como o próprio BigChainDB. O MongoDB Compass é útil para visualizar as movimentações no banco de dados.

Como descrito anteriormente, os *scripts* em Python têm a exclusiva finalidade de executar comandos no terminal. Por isso, nos tópicos a seguir, apenas serão explicitados os comandos, em vez de todo o código de cada *script*. O código completo pode ser consultado no repositório público do autor[4].

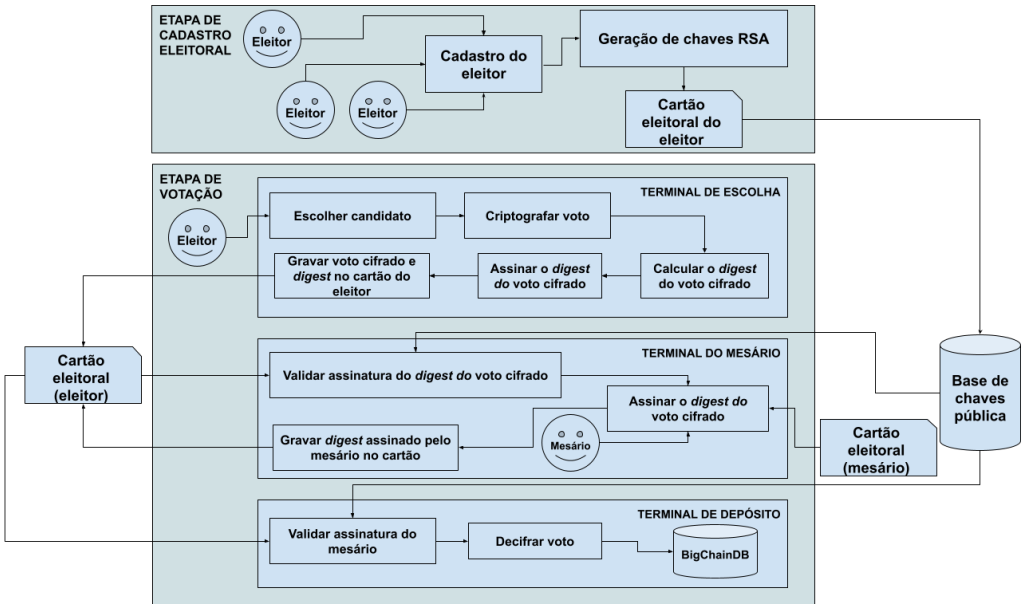

Figura 7 - Diagrama de blocos do sistema

O diagrama da Figura 7 representa o sistema como foi implementado. Os códigos dos tópicos a seguir estão descritos da maneira como foram organizados em cada máquina virtual, e não em uma sequência de execução. A sequência

[3] https://www.mongodb.com/products/compass

[4] lpinto39/blockchain-voting (github.com)

de execução está demonstrada no Capítulo 6, da prova de conceito.

5.1 Servidor central da instituição

Nesta máquina virtual, são registrados os dados do eleitor. Os dados de interesse para esta proposta são o número de inscrição do eleitor associado à sua chave pública. O *script* executa a seguinte sequência de comandos:

```
1. openssl genrsa -aes-256-cbc -out
   pendrive/XXXXXXXXXXXX_private.pem 4096
2. openssl rsa -in pendrive/XXXXXXXXXXXX_private.pem -pubout –out
   XXXXXXXXXXXX_public.pem
```

onde XXXXXXXXXXXX é o número de inscrição do eleitor. A primeira linha representa a geração de uma chave privada (`pendrive/XXXXXXXXXXXX_private.pem`) protegida por senha requerida pelo usuário, que deve ser introduzida no terminal. A segunda linha, a exportação da sua chave pública (`XXXXXXXXXXXX_public.pem`). A chave pública é armazenada em um diretório público, enquanto a chave privada é armazenada no cartão eleitoral.

Cabe enfatizar que o mesário também é um eleitor, ou seja, a ele também é gerado um par de chaves pública e privada. Porém, no caso do mesário, este par de chaves também terá utilidade ao manusear o terminal do mesário. Este processo será mais bem detalhado no tópico seguinte.

Esta máquina virtual também é responsável por executar o algoritmo Diffie-Hellman, que resultará em uma *chave global* (`chave-global.pem`), que também estará armazenada em um diretório do servidor. Este passo é executado após finalizada a etapa de cadastro dos eleitores, em outro *script*, com o comando abaixo:

```
1. openssl genpkey -genparam -algorithm DH -out chave-global.pem
```

Posteriormente, esta *chave global* será armazenada nos terminais de votação, de modo a manter uma sincronização segura entre elas. Este é um processo manual, que deve ser realizado a cada nova eleição e permite que os

demais terminais prossigam com a sua própria configuração.

5.2 Terminal de escolha do candidato

Este é o terminal onde o eleitor realiza a escolha do(s) seu(s) candidato(s) para o(s) respectivo(s) cargo(s) em disputa. Como configuração inicial, antes do início das votações, gera-se uma chave privada (`privTEscolha.pem`) e se exporta a sua respectiva chave pública (`pendriveSeção/publicTEscolha.pem`), conforme as duas linhas de comando a seguir.

```
1. openssl genpkey -param file pendriveSeção/chave-global.pem -out
   privTEscolha.pem
2. openssl pkey -in privTEscolha.pem -pubout -out
   pendriveSeção/publicTEscolha.pem
```

A *chave global* (`pendriveSeção/chave-global.pem`) do servidor central, foi previamente transferida para este terminal, pois este é utilizado como parâmetro para a chave privada.

Nesta máquina ocorre o processo de derivação das chaves privada do terminal de escolha com a chave pública do terminal de depósito. O objetivo deste processo é criptografar a troca de informações entre os dois terminais. Para isso, antes da execução do comando abaixo, a chave pública do terminal de depósito (`pendriveSeção/publicTDeposito.pem`) é utilizada. O produto deste comando é um arquivo binário (`keyTEscolhaTDeposito.bin`).

```
1. openssl pkeyutl -derive -inkey privTEscolha.pem -peerkey
   pendriveSeção/publicTDeposito.pem -out keyTEscolhaTDeposito.bin
```

Para a etapa em que as votações estão abertas e o eleitor pode fazer a escolha do seu candidato, executa-se o comando a seguir:

```
1. openssl aes-256-cbc -e -kfile keyTEscolhaTDeposito.bin -out
   pendrive/voto-secreto.bin <<< XX
```

onde XX é o número do candidato escolhido pelo eleitor. Este comando utiliza

como parâmetro o arquivo binário criado na derivação das chaves, no comando anterior. A saída desta execução é um arquivo binário com a informação do voto do eleitor (`pendrive/voto-secreto.bin`).

Nesta etapa o voto foi cifrado com o AES em modo de operação CBC (*cipher-block chaining*), que garante um vetor de inicialização aleatório, assim dois votos iguais possuem um arquivo (`pendrive/voto-secreto.bin`) de saída totalmente diferente. Para esta implementação, considera-se que existe apenas um cargo em disputa na eleição.

Para realizar a assinatura cega do voto, os dois comandos a seguir são executados:

```
1. sha512sum pendrive/voto-secreto.bin > pendrive/voto-
   secreto.hash
2. openssl dgst -sha512 -sign pendrive/XXXXXXXXXXXX_private.pem -
   out pendrive/voto-secreto.sign pendrive/voto-secreto.hash
```

Na primeira linha, calcula-se o *message digest* com a função hash SHA-512 do arquivo (`pendrive/voto-secreto.bin`), que contém a informação da escolha do eleitor, isto é, se o eleitor escolheu, por exemplo, o candidato de número 91, este valor será transformado em uma cadeia de 512 caracteres no arquivo gerado a partir deste comando (`pendrive/voto-secreto.hash`). Se qualquer outro eleitor, desta ou de outra seção eleitoral, também escolher o candidato de número 91, a cadeia de 512 caracteres será distinta, uma vez que foi utilizado o AES em modo CBC. Este arquivo com o *message digest* (`pendrive/voto-secreto.hash`) do voto é assinado pelo eleitor, conforme ocorre na linha seguinte.

Através do *message digest* não é possível saber o voto, então, trata-se de uma assinatura cega. Para a assinatura, utiliza-se a chave privada do eleitor (`pendrive/XXXXXXXXXXXX_private.pem`) e a saída é o arquivo assinado (`pendrive/voto-secreto.sign`), por isso também é gerado um arquivo com a extensão *SIGN*. Este arquivo se mantém armazenado no cartão eleitoral.

5.3 Terminal do mesário

Primeiramente, cabe ressaltar que o terminal do mesário não pode ser confundido com a pessoa que atua como mesário (e esta, por sua vez, também é um eleitor). No terminal do mesário, deve ser gerado um par de chaves pública e privada, durante a configuração para as eleições, conforme o comando abaixo:

```
1. openssl genpkey -paramfile pendriveSeção/chave-global.pem -out
   privTMesa.pem
2. openssl pkey -in chave-privada-mesa.pem -pubout -out
   pendriveSeção/publicTMesa.pem
```

Os comandos acima, respectivamente, geram uma chave privada (`privTMesa.pem`) e uma chave pública (`pendriveSeção/publicTMesa.pem`) para o terminal do mesário. A chave privada do terminal, em especial, utiliza como parâmetro a *chave global* da eleição em questão, a mesma que foi gerada no servidor central. Como descrito no tópico anterior, a *chave global* é enviada para cada uma das demais máquinas através de um dispositivo removível (`pendriveSeção`).

O terminal do mesário é responsável por validar a assinatura do eleitor (`pendrive/voto-secreto.sign)` que foi gerada a partir do *message digest* do voto (`pendrive/voto-secreto.hash`). Este processo é mais bem descrito no próximo tópico.

O *message digest* do voto é recebido via cartão eleitoral e, então, realiza-se a verificação da assinatura do eleitor e a assinatura do *message digest* do voto pelo mesário, conforme as duas linhas seguintes:

```
1. openssl dgst -sha512 -verify XXXXXXXXXXXX_public.pem -signature
   pendrive/voto-secreto.sign pendrive/voto-secreto.hash
2. openssl dgst -sha512 -sign pendriveMesario/YYYYYYYYYY_private.pem
   -out pendrive/voto-secreto.sign pendrive/voto-secreto.hash
```

Na primeira linha, a chave pública do eleitor (`XXXXXXXXXXXX_public.pem`) é utilizada para confirmar que o *message digest* do voto (`pendrive/voto-`

`secreto.hash`) foi assinado (`pendrive/voto-secreto.sign`) pela mesma pessoa que o apresentou. A chave pública do eleitor está previamente armazenada no terminal do mesário.

O comando responde se a verificação foi bem-sucedida ou não. Já na segunda linha, realiza-se a assinatura cega do voto do eleitor, uma vez que o mesário irá assinar o *message digest* do voto (`pendrive/voto-secreto.hash`) sem ter conhecimento ou acesso ao conteúdo do voto. Para isso, o parâmetro de entrada é a chave privada do mesário (`pendriveMesario/YYYYYYYYY_private.pem`), onde YYYYYYYYY é o número de inscrição do título de eleitor do mesário.

5.4 Terminal de depósito do voto

Este terminal também possuirá o seu próprio par de chaves pública (`pendriveSeção/publicTDeposito.pem`) e privada (`privTDeposito.pem`), geradas em um processo idêntico ao que ocorreu nos terminais citados nos tópicos anteriores, mas atribuindo, aos arquivos de cada uma das chaves, um nome correspondente a este terminal, conforme os comandos a seguir.

```
1. openssl genpkey -paramfile pendriveSeção/chave-global.pem -out
   privTDeposito.pem
2. openssl pkey -in privTDeposito.pem -pubout -out
   pendriveSeção/publicTDeposito.pem
```

Novamente, a *chave global* (`pendriveSeção/chave-global.pem`), gerada no servidor central, para sincronização, deve ser utilizada para esta máquina, pois esta é utilizada como parâmetro para gerar a chave privada, de modo a garantir a sincronização segura das máquinas.

Nesta máquina ocorre novamente o processo de derivação das chaves privada do terminal de escolha com a chave pública do terminal de depósito. O objetivo deste processo é criptografar a troca de informações entre os dois terminais. Para isso, antes da execução do comando abaixo, a chave pública do terminal de depósito (`pendriveSeção/publicTEscolha.pem`) é utilizada. O produto deste comando é um arquivo binário (`keyTEscolhaTDeposito.bin`).

```
1. openssl pkeyutl -derive -inkey privTDeposito.pem -peerkey
   pendriveSeção/publicTEscolha.pem -out keyTEscolhaTDeposito.bin
```

Este terminal será utilizado para depositar o voto do eleitor, somente após a realização da escolha e das assinaturas cegas, tanto pela parte do eleitor como pela parte do mesário. O arquivo que contém a informação do voto (`pendrive/voto-secreto.bin`) será acessado via cartão eleitoral, quando inserido neste terminal. Nesta etapa, realiza-se uma verificação da assinatura do mesário (o eleitor não precisa verificar a sua própria assinatura, pois esta etapa já foi realizada pelo mesário em seu terminal).

```
1. sha512sum pendrive/voto-secreto.bin > validacao
2. openssl dgst -sha512 -verify YYYYYYYYY_public.pem -signature
   pendrive/voto-secreto.sign validacao
3.  PythonScript << openssl aes-256-cbc -pbkdf2 -d -kfile
   keyTEscolhaTDeposito.bin -in pendrive/voto-secreto.bin
```

Na primeira linha, um novo *message digest* é calculado com a função *hash* SHA-512, que tem uma saída o arquivo de validação (`validacao`) para realizar a comparação. Isso evita que o voto seja alterado durante o processo.

Na linha seguinte, isto é, verificar a correspondência com o arquivo recebido pelo mesário e confirmar a sua assinatura. Qualquer inconsistência nesta etapa, o comando indica um erro na tela do terminal. Na última linha, a partir do arquivo gerado na derivação entre o terminal da escolha e o terminal do depósito (`keyTEscolhaTDeposito.bin`), utilizado como parâmetro, o eleitor é capaz de visualizar, de maneira clara, o número do candidato em quem ele votou.

Por fim, se todas as etapas do processo ocorrerem bem, um *script* Python é responsável por guardar o voto do eleitor no banco de dados BigChainDB. Por se tratar de uma única seção eleitoral, com um único terminal de depósito do voto, então a totalização dos votos é realizada diretamente nesta máquina. Para isso, os votos podem ser visualizados a partir do MongoDB Compass.

6 Prova de conceito

Como prova de que a implementação do sistema funciona, foi simulado um processo de votação dentro do ambiente especificado na implementação, com dois eleitores fictícios, sendo um deles o mesário, além de seis candidatos fictícios.

O primeiro passo do processo ocorre durante a etapa de cadastro eleitoral, isto é, quando os eleitores devem procurar um cartório eleitoral para registrar ou atualizar os seus dados.

Nesta etapa, ao fornecer o número de inscrição, que consta no título de eleitor, o eleitor deve, também, criar uma senha para o seu certificado eleitoral (a sua chave privada). Em seguida, uma chave pública também é criada, para qual é solicitada a senha da sua chave privada correspondente. Ao fim, o eleitor recebe, junto ao seu documento, um dispositivo removível (o seu cartão eleitoral) contendo o seu certificado eleitoral, que não pode ser compartilhado e deve ser acessado somente mediante senha em uma seção eleitoral. Já a chave pública do eleitor, mantém-se registrada na máquina que representa o servidor central da instituição autárquica eleitoral.

Dois eleitores foram registrados, sendo um deles, o mesário. A seguir, descreve-se o processo de votação que deve ser cumprido pelos eleitores.

Figura 8 - Geração do par de chaves pública e privada do eleitor

Finalizada a etapa do cadastro, a instituição eleitoral pode iniciar a

configuração dos terminais que estarão disponíveis na seção eleitoral, a saber: o terminal do mesário, a urna de escolha do candidato do eleitor e a urna de depósito do voto do eleitor. Para garantir a segurança da informação do voto entre os terminais, o algoritmo Diffie-Hellman é executado no sistema central e, como produto, uma *chave global* é gerada. Este processo pode levar alguns minutos.

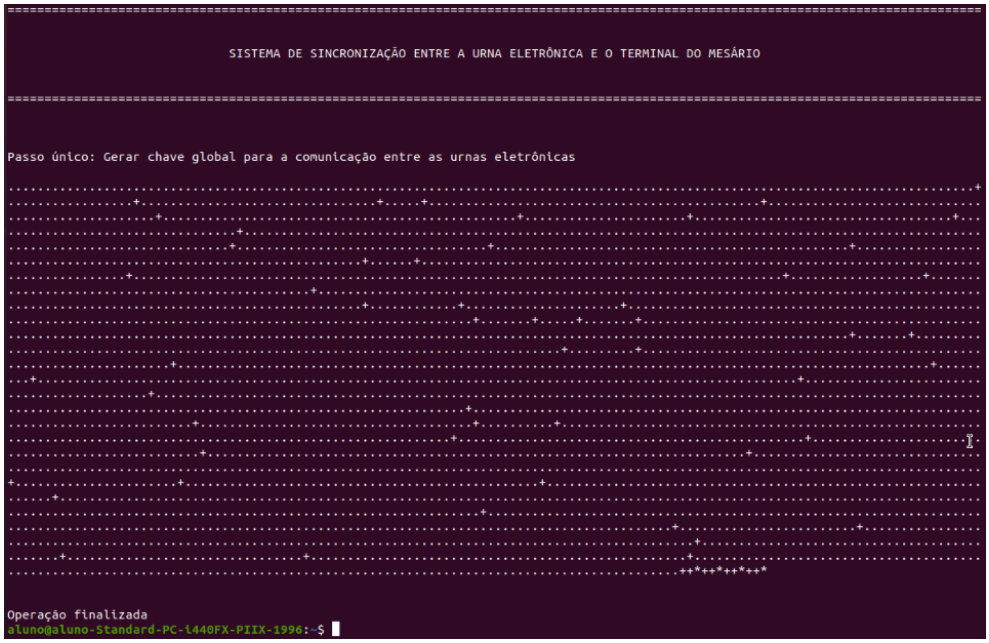

Figura 9 - Execução do algoritmo Diffie-Hellman, que gera uma chave global

Esta chave deve ser transferida do sistema central para cada terminal das seções eleitorais através de um dispositivo removível (como um *pendrive*). Logo, cada um dos três terminais da seção eleitoral deve, individualmente, gerar o seu próprio par de chaves pública e privada, conforme a Figura 10.

Figura 10 - Geração do par de chaves pública e privada do terminal

Além disso, em seguida, também se realiza a derivação das chaves da urna de escolha e da urna de depósito para que a informação do voto esteja legível nestes terminais e estritamente nestes terminais.

Estes passos garantem que, ao abrir as votações, não haverá (a) fuga de informação, (b) interceptação de dados por terceiros, (c) interação do eleitor ou mesário com terminais *fake* e (d) dependência da disposição do eleitor em ser honesto para garantir a segurança da informação do processo.

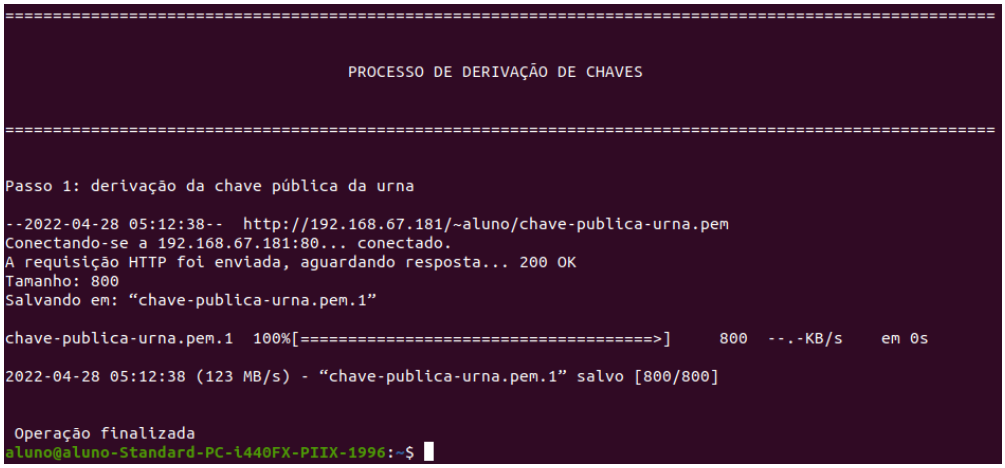

Figura 11 - Derivação entre as chaves do terminal de depósito e o terminal de escolha

Por fim, a chave pública do eleitor também é transferida do sistema central para a urna de escolha do eleitor em sua respectiva seção eleitoral, além do terminal do mesário, para confirmar sua identidade. O processo descrito neste parágrafo deve ocorrer em cada nova eleição.

Com os terminais da seção eleitoral em questão devidamente configurados e sincronizados, a etapa de votação pode ser iniciada. Dentro da seção eleitoral, o eleitor deve se dirigir ao terminal de escolha para selecionar o seu candidato. Neste momento, o eleitor deve injetar o seu cartão eleitoral na urna.

O primeiro a votar foi o mesário, escolhido o candidato Wadenhad, de número 91. Para o outro eleitor, foi escolhido o candidato Nimba, de número 95.

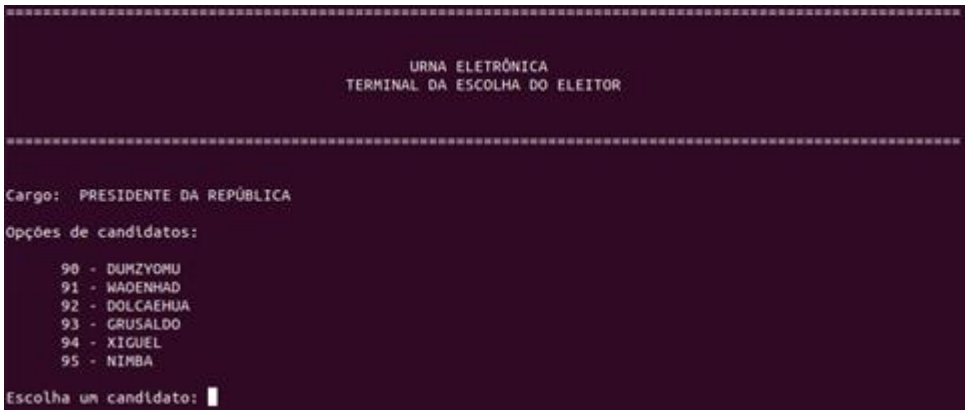

Figura 12 - Representação da tela de escolha do candidato pelo eleitor, com nomes fictícios

Quando selecionado o candidato, o eleitor deve assinar o seu voto e, então, gera-se um *message digest* referente ao seu voto, ou seja, ocorre o primeiro passo para a assinatura cega. Este arquivo estará armazenado no cartão eleitoral. Por fim, o eleitor deve remover o seu cartão eleitoral e se dirigir ao mesário.

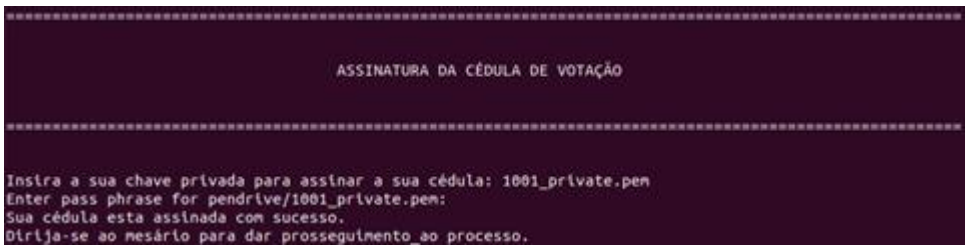

Figura 13 - Assinatura da cédula do voto pelo eleitor, após realizar a sua escolha

O mesário deve solicitar que o eleitor insira o cartão eleitoral no seu terminal para validar a assinatura do voto. Se a validação for bem-sucedida, isto é, se o voto assinado corresponde à pessoa que o apresentou, então o mesário pode assinar este voto do eleitor. Este é o último passo para a assinatura cega. Caso a validação não seja bem-sucedida, uma mensagem de erro é exibida na tela. O voto assinado pelo mesário é exatamente o arquivo codificado mencionado no parágrafo anterior, logo o mesário não é capaz de saber o conteúdo da escolha do eleitor. Ao fim, o eleitor pode ejetar o seu cartão eleitoral do terminal do mesário.

Depois de assinado pelas duas partes, o voto do eleitor pode, finalmente, ser enviado para a urna de depósito. Então, o eleitor deve inserir o seu cartão eleitoral nesta urna e, em seguida, também pode verificar a assinatura do

mesário. Caso nenhuma mensagem de erro seja exibida na tela, isto é, se a validação é bem-sucedida, o eleitor pode, finalmente, confirmar o seu voto. Ao confirmar o voto, este será guardado no BigChainDB, instalado nesta mesma urna.

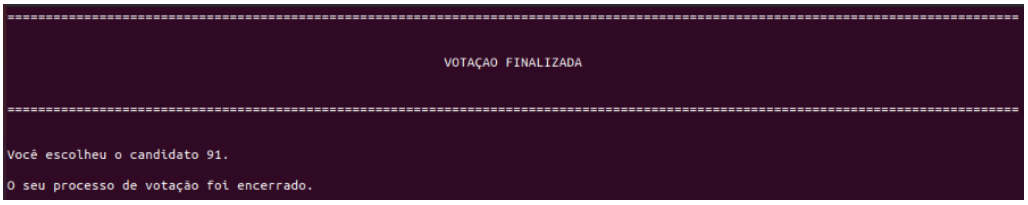

Figura 14 - Processo de votação do eleitor concluído

Quando a mensagem que indica o fim da votação do eleitor é exibida na tela, o cartão eleitoral pode ser removido da urna e guardado para a próxima eleição. A partir deste momento, nenhuma outra etapa é exigida do eleitor, que pode se retirar da seção eleitoral.

Considerando-se o fim das votações, a apuração do resultado pode ser realizada. Então, através do MongoDB Compass, os votos depositados na urna podem ser consultados.

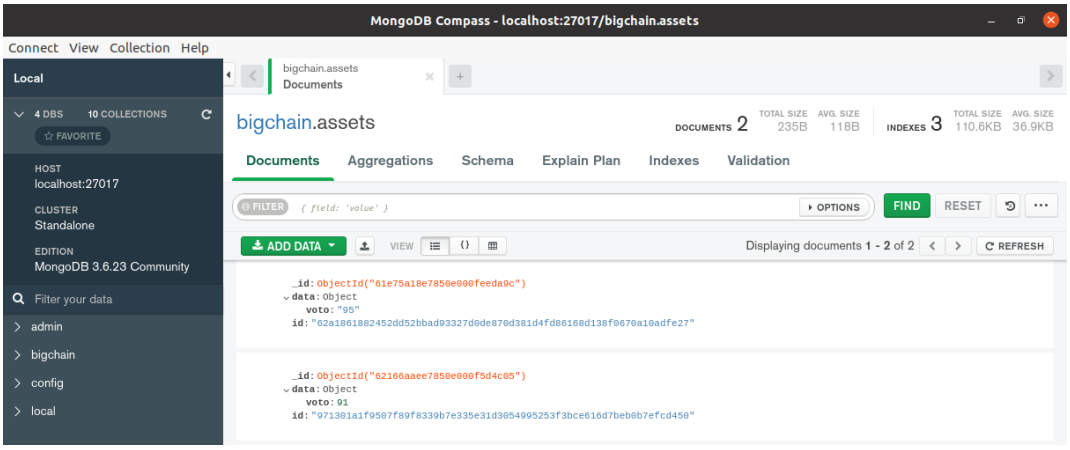

Figura 15 - Votos dos eleitores registrados no BigChainDB

Os votos dos dois eleitores estão registrados no banco de dados e humanamente legíveis para permitir a apuração pública dos resultados. Portanto, todo o processo desenvolvido, desde o cadastro eleitoral até a totalização dos votos funcionou como desejado.

7 Conclusão

Neste artigo, foi discutido, brevemente, o funcionamento do atual processo eleitoral brasileiro e os seus desafios, a partir uma perspectiva técnica, tanto no aspecto da tecnologia da informação, como também no aspecto jurídico, que são fontes para inspirar outros trabalhos com propostas de solução aos problemas levantados aqui. Afinal, este artigo possui o escopo limitado à segurança da informação, e, mesmo assim, não é possível solucionar todos os seus problemas aplicados ao contexto eleitoral.

A proposta apresentada neste trabalho permite que o eleitor seja capaz de validar o seu voto sem que, ao mesmo tempo, gere qualquer evidência da sua escolha, de modo não apenas satisfazer a Constituição Federal, como também garantir segurança ao eleitor no sigilo absoluto da sua escolha. O funcionamento da proposta apresentada exige modificações no processo eleitoral brasileiro, especialmente na etapa da votação, com o acréscimo novos passos e dispositivos no processo atual, mas segue com a garantia do voto digital e desconectado de redes de Internet.

Com o sistema, pode-se realizar uma auditoria das eleições a qualquer tempo após o término das votações, uma vez que os arquivos criptografados do voto se mantêm armazenados no dispositivo do eleitor. Portanto, cumpre com o objetivo em solucionar o problema descrito na introdução deste artigo, em como garantir uma eleição que seja (a) 100% digital, (b) com votos anônimos e (c) publicamente auditável. Entretanto, também como definido no objetivo, este trabalho não tratou de definir um processo de auditoria, mas apenas de possibilitá-lo, tal como requisitado. Para trabalhos futuros, pode-se realizar um estudo aprofundado sobre auditoria em sufrágios políticos, de modo a desenvolver um processo adequado a este sistema.

REFERÊNCIAS

ADIPUTRA, C. K.; HJORT, R.; SATO, H. A Proposal of Blockchain-Based Electronic Voting System. *In*: , 2018. **2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)**. [*S. l.: s. n.*], 2018. p. 22–27.

ASHIDANI, P. J.; BARBAR, J. S. **Criptografia para Voz sobre IP com Curvas Elípticas**. 2008. 7 f. Mestrado - Universidade Federal de Uberlandia, Uberlândia, 2008. Disponível em: http://www.facom.ufu.br/posgrad/WD1/pedro.pdf. Acesso em: 15 jan. 2022.

BARROS, C. F. de; PIMENTA, D. F. A Receipt-Free i-Voting System Based on Blind Signatures and Anonymous IDs. *In*: , 2018, Porto Alegre, RS, Brasil. **Anais do XVIII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais**. Porto Alegre, RS, Brasil: SBC, 2018. p. 113–120. Disponível em: https://sol.sbc.org.br/index.php/sbseg/article/view/4277.

BIGCHAINDB GMBH. **BigchainDB 2.0, The Blockchain Database**. 2018. Berlim, 2018. Disponível em: https://www.bigchaindb.com/whitepaper/bigchaindb-whitepaper.pdf. Acesso em: 26 out. 2021.

BRASIL. **Cadastro de eleitores**. [*S. l.*], 2015a. Disponível em: https://www.tse.jus.br/eleicoes/processo-eleitoral-brasileiro/cadastro-de-eleitores/cadastro-eleitoral. Acesso em: 29 nov. 2021.

BRASIL. **Título Net já registra quase 420 mil solicitações por serviços da Justiça Eleitoral**. [*S. l.*], 2020. Disponível em: https://www.tse.jus.br/imprensa/noticias-tse/2020/Maio/titulo-net-ja-registra-quase-420-mil-solicitacoes-por-servicos-da-justica-eleitoral. Acesso em: 21 out. 2021.

BRASIL. **Totalização dos resultados das eleições**. [*S. l.*], 2015b. Disponível em: https://www.tse.jus.br/eleicoes/processo-eleitoral-brasileiro/totalizacao/totalizacao-dos-resultados-das-eleicoes. Acesso em: 29 nov. 2021.

BRASIL. **Urna eletrônica: 20 anos a favor da democracia**. [*S. l.*]: Tribunal Superior Eleitoral, 2016. Disponível em: https://bibliotecadigital.tse.jus.br/xmlui/handle/bdtse/1935. Acesso em: 21 out. 2021.

BRASIL. **Votação**. [*S. l.*], 2015c. Disponível em: https://www.tse.jus.br/eleicoes/processo-eleitoral-brasileiro/votacao/votacao-totalizacao-e-divulgacao-de-resultados. Acesso em: 29 nov. 2021.

CHAUM, D. Blind Signatures for Untraceable Payments. **Springer, Boston, MA**, [*s. l.*], 1983. Disponível em:

https://sceweb.sce.uhcl.edu/yang/teaching/csci5234WebSecurityFall2011/Chaum-blind-signatures.PDF.

DANG, Q. **Secure Hash Standard (SHS)**. [*S. l.: s. n.*], 2015. Disponível em: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf. Acesso em: 18 fev. 2021.

DWORKING, M. *et al.* **Advanced Encryption Standard (AES)**. [*S. l.: s. n.*], 2001. Disponível em: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf. Acesso em: 18 fev. 2021.

JÚNIOR, E. F. El mito del secreto bancario ante el fisco: el caso de Brasil. **Revista de Administración Tributaria**, [*s. l.*], p. 53–78, 2016.

KOERIG, J. H. A desinformação no processo eletrônico de votação: uma análise sob o aspecto da competência informacional do indivíduo. **Revista Científica Multidisciplinar**, [*s. l.*], p. 5–21, 2021.

KUMAR, D. A.; BEGUM, T. U. S. Electronic voting machine — A review. *In*: , 2012. **International Conference on Pattern Recognition, Informatics and Medical Engineering (PRIME-2012)**. [*S. l.: s. n.*], 2012. p. 41–48.

MARCACINI, A. T. R.; BARRETO JUNIOR, I. F. Aspectos jurídicos, políticos e técnicos sobre sistemas eletrônicos de votação e a urna eletrônica brasileira. **Revista Brasileira de Estudos Políticos**, [*s. l.*], v. 118, 2019. Disponível em: https://pos.direito.ufmg.br/rbep/index.php/rbep/article/view/696. Acesso em: 29 jul. 2021.

NAKAMOTO, S. **Bitcoin: A Peer-to-Peer Electronic Cash System**. 2008. 9 f. [*s. l.*], 2008. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 11 dez. 2021.

OLIVEIRA, F. M. de. **A transparência e a auditoria da urna eletrônica: a soberania popular materializada na legitimidade do voto**. 2021. 114 f. - Universidade Federal do Ceará, Fortaleza, 2021. Disponível em: http://www.repositorio.ufc.br/handle/riufc/57982.

OSGOOD, R. The future of democracy: Blockchain voting. **COMP116: Information security**, [*s. l.*], p. 1–21, 2016.

STALLINGS, W. **Criptografia e segurança de redes: princípios e práticas**. 6. ed. São Paulo: Pearson Education do Brasil, 2015.

XU, M.; CHEN, X.; KOU, G. A systematic review of blockchain. **Financial Innovation**, [*s. l.*], n. 5, 2019. Disponível em: https://link.springer.com/content/pdf/10.1186/s40854-019-0147-z.pdf.

LAZARIN, N. M. **Método não supervisionado de reconhecimento de padrões criptográficos**. 2012. 75 f. - Instituto Militar de Engenharia, Rio de Janeiro, 2012.

Disponível em: http://www.comp.ime.eb.br/pos/modules/files/dissertacoes/2012/2012-Nilson.pdf.